Course 6421A:
Configuring and Troubleshooting a
Windows Sever 2008 Network Infrastructure

About this Course
This five-day instructor-led course provides students with the knowledge and skills to configure and troubleshoot a Windows Sever 2008 network infrastructure. Students will learn to implement and configure secure network access and implement fault tolerant storage technologies. Students will gain an understanding of the network technologies most commonly used with Windows Server 2008 and IP-enabled networks. Students will also learn how to secure servers and maintain update compliance.

Audience Profile
The primary audience for this course includes Active Directory technology specialists aspiring to be Enterprise Administrators (Tier 4 day-to-day network operations) or Network Administrators (Tier 2). Experienced Server Administrators aspiring to be Enterprise Administrators would also benefit from this course.
The secondary audience for this course includes Storage Area Network Administrators who need to understand this information to deploy or extend their current storage infrastructure. Operations Managers who need this information to support troubleshooting efforts and business decisions would also benefit from this course.

At Course Completion
After completing this course, students will be able to:
- Install and configure servers.
- Configure and troubleshoot DNS.
- Configure and manage WINS.
- Configure and troubleshoot DHCP.
- Configure and troubleshoot IPv6 TCP/IP.
- Configure and troubleshoot Routing and Remote Access.
- Install, configure, and troubleshoot the Network Policy Server Role service.
- Configure Network Access Protection.
- Configure IPsec.
- Monitor and troubleshoot IPsec.
- Configure and manage Distributed File System.
- Configure and manage storage technologies.
- Configure availability of network resources and content.
- Configure server security compliance.

Prerequisites
Before attending this course, students must have:
- Working experience with Windows Server 2003.
- Basic knowledge of Active Directory.
- An understanding of security concepts and methodologies (for example, corporate policies).
- Basic knowledge of DHCP.
- Basic knowledge of IPsec.

Course Outline

Module 1: Installing and Configuring Servers
This module explains how to identify the appropriate usage scenario and installation type for a server and then install and configure appropriate server roles and features.
Lessons

- Installing Windows Server 2008
- Managing Server Roles and Features
- Overview of the Server Core Installation Option

Lab: Installing and Configuring Servers and Server Roles
Exercise 1: Identifying Server Types
Exercise 2: Installing and Configuring Server Roles and Features
Exercise 3: Configuring Server Core and Performing Basic Management Tasks
After completing this module, students will be able to:
Identify the system requirements and process for installing Windows Server 2008.
Describe the difference between server roles and features.
Describe the benefits of and roles supported by a Server Core installation.

Module 2: Configuring and Troubleshooting DNS
This module explains how to configure, manage and troubleshoot DNS server and zone properties to be used in a secure environment.
Lessons

- Installing the DNS Server Role
- Configuring the DNS Server Role
- Configuring DNS Zones
- Configuring DNS Zone Transfers
- Managing and Troubleshooting DNS

Lab: Configuring and Verifying a DNS Solution
Exercise 1: Configuring a DNS Infrastructure
Exercise 2: Monitoring and Troubleshooting DNS
After completing this module, students will be able to:
Install the DNS Server role.
Configure the DNS Server role to support various query types.
Configure DNS zones.
Configure DNS zone transfers.
Manage DNS zone records and troubleshoot DNS using various tools.

Module 3: Configuring and Managing WINS
This module explains how to configure, manage and troubleshoot WINS servers.
Lessons

- Overview of the Windows Internet Name Service
- Managing the WINS Server
- Configuring WINS Replication
- Migrating from WINS to DNS

Lab: Configuring a WINS Infrastructure
Exercise 1: Installing WINS
Exercise 2: Configuring WINS Burst Handling
Exercise 3: Configuring WINS Replication
Exercise 4: Migrating from WINS to DNS
After completing this module, students will be able to:

Install and configure the Windows Internet Name Service.
Manage WINS client records.
Configure and manage WINS replication.
Migrate a WINS infrastructure to DNS.

Module 4: Configuring and Troubleshooting DHCP
This module explains how to configure, manage and troubleshoot a DHCP environment supporting an IPV4 infrastructure.
Lessons

- Overview of the DHCP Server Role
- Configuring DHCP Scopes and Options
- Managing a DHCP Database
- Monitoring and Troubleshooting DHCP
- Securing DHCP

Lab: Configuring and Troubleshooting the DHCP Server Role
Exercise 1: Installing and Authorizing the DHCP Server Role
Exercise 2: Configuring a DHCP Scope
Exercise 3: Troubleshooting Common DHCP Issues
After completing this module, students will be able to:
Describe how DHCP works.
Configure DHCP scopes and options.
Manage a DHCP database.
Monitor and troubleshoot DHCP.
Secure DHCP.

Module 5: Configuring and Troubleshooting IPv6 TCP/IP
This module explains how to configure and troubleshoot static and dynamic IPv6 addresses, including subnet prefix lengths, gateways and DNS servers.
Lessons

- Overview of IPv6
- Coexistence with IPv6
- IPv6 Tunneling Technologies
- Transitioning from IPv4 to IPv6
- Troubleshooting IPv6

Lab A: Configuring an ISATAP Router
Exercise 1: Configuring a New IPv6 Network and Client
Exercise 2: Configuring an ISATAP Router to Enable Communication Between an IPv4 Network and an IPv6 Network
Lab B: Converting the Network
Exercise 1: Transitioning to an IPv6-Only Network
After completing this module, students will be able to:
Describe the benefits and considerations of IPv6.
Describe how IPv6 can coexist with IPv4 environments.
Describe IPv6 tunneling technologies used to interoperate with IPv4 networks.
Describe the process used to migrate from IPv4 to IPv6.
Troubleshoot IPv6 connectivity.

Module 6: Configuring and Troubleshooting Routing and Remote Access
This module explains how to configure and troubleshoot Routing and Remote Access Services.
Lessons

- Configuring Network Access
- Configuring VPN Access
- Overview of Network Policies
- Overview of the Connection Manager Administration Kit
- Troubleshooting Routing and Remote Access

Lab: Configuring and Managing Network Access

Exercise 1: Configuring Routing and Remote Access as a VPN Remote Access Solution
Exercise 2: Configuring a Custom Network Policy
Exercise 3: Configuring Logging
Exercise 4: Configuring a Connection Profile
After completing this module, students will be able to:
Install and configure the Routing and Remote Access service.
Configure VPN access.
Configure network policies.
Configure a connection profile using the Connection Manager Administration Kit.
Troubleshoot Routing and Remote Access.

Module 7: Installing, Configuring, and Troubleshooting the Network Policy Server Role Service

This module explains how to install, configure and troubleshoot the Network Policy Server Role service.

Lessons

- Installing and Configuring a Network Policy Server
- Configuring RADIUS Clients and Servers
- NPS Authentication Methods
- Monitoring and Troubleshooting a Network Policy Server

Lab: Configuring and Managing Network Policy Server

Exercise 1: Installing and Configuring the Network Policy Server Role Service
Exercise 2: Configuring a RADIUS Client
Exercise 3: Configuring Certificate Auto-Enrollment
After completing this module, students will be able to:
Install and configure the Network Policy Server role.
Configure a RADIUS client and server.
Describe NPS authentication methods.
Monitor and troubleshoot a Network Policy server.

Module 8: Configuring Network Access Protection

This module explains how to configure and manage NAP for DHCP, VPN, and 802.1X.

Lessons

- Overview of Network Access Protection
- How NAP Works
- Configuring NAP
- Monitoring and Troubleshooting NAP

Lab: Configuring NAP for DHCP and VPN

Exercise 1: Configuring NAP for DHCP Clients
Exercise 2: Configuring NAP for VPN Clients
After completing this module, students will be able to:
Describe the benefits and uses of NAP.

Describe how NAP works in various access scenarios.
Configure NAP.
Monitor and troubleshoot NAP.

Module 9: Configuring IPsec
This module explains how to configure and test IPsec.
Lessons

- Overview of IPsec
- Configuring Connection Security Rules
- Configuring IPsec NAP Enforcement

Lab: Configuring IPsec NAP Enforcement
Exercise 1: Preparing the Network Environment for IPsec NAP Enforcement
Exercise 2: Configuring and Testing IPsec NAP Enforcement
After completing this module, students will be able to:
Describe the benefits and uses of IPsec.
Configure Connection Security rules.
Configure IPsec NAP enforcement.

Module 10: Monitoring and Troubleshooting IPsec
This module explains how to monitor and troubleshoot IPsec.
Lessons

- Monitoring IPsec Activity
- Troubleshooting IPsec

Lab: Monitoring and Troubleshooting IPsec
Exercise 1: Monitoring IPSec Connectivity
Exercise 2: Configuring Connection Security
Exercise 3: Troubleshooting IPSec
After completing this module, students will be able to:
Monitor IPsec activity.
Troubleshoot IPsec.

Module 11: Configuring and Managing Distributed File System
This module explains how to configure and manage Distributed File System.
Lessons

- DFS Overview
- Configuring DFS Namespaces
- Configuring DFS Replication

Lab: Configuring DFS
Exercise 1: Installing the Distributed File System Role Service
Exercise 2: Creating a DFS Namespace
Exercise 3: Configuring Folder Targets and Folder Replication
Exercise 4: Viewing Diagnostic Reports for Replicated Folders
After completing this module, students will be able to:
Describe the Distributed File System.
Manage DFS namespaces.
Configure DFS replication.

Module 12: Configuring and Managing Storage Technologies
This module explains how to configure and troubleshoot file system storage technologies included with Windows Server 2008.
Lessons

- Windows Server 2008 Storage Management Overview
- Managing Storage Using File Server Resource Manager
- Configuring Quota Management
- Implementing File Screening
- Managing Storage Reports

Lab: Configuring and Managing Storage Technologies
Exercise 1: Installing the FSRM Role Service
Exercise 2: Configuring Storage Quotas
Exercise 3: Configuring File Screening
Exercise 4: Generating Storage Reports
After completing this module, students will be able to:
Describe storage management solutions included in Windows Server 2008.
Manage storage using File Server Resource Manager (FSRM).
Configure quota management using FSRM.
Implement file screening using FSRM.
Manage storage reports.

Module 13: Configuring Availability of Network Resources and Content
This module explains how to describe and configure backup and recovery methods.
Lessons

- Backing Up Data
- Configuring Shadow Copies
- Providing Server and Service Availability

Lab: Configuring Availability of Network Resources
Exercise 1: Configuring Windows Server Backup and Restore
Exercise 2: Configuring Shadow Copying
Exercise 3:Configuring Network Load Balancing
After completing this module, students will be able to:
Back up data.
Configure shadow copies.
Provide server and service availability.

Module 14: Configuring Server Security Compliance
This module explains how to configure and analyze server security and security update compliance.
Lessons

- Securing a Windows Infrastructure
- Using Security Templates to Secure Servers
- Configuring an Audit Policy
- Overview of Windows Sever Update Services
- Managing WSUS

Lab: Configuring Server Security Compliance
Exercise 1: Configuring and Analyzing Security
Exercise 2: Analyzing Security Templates

Exercise 3: Configuring Windows Software Update Services
After completing this module, students will be able to:
Secure a server role within a Windows infrastructure.
Secure servers using security templates.
Configure an audit policy.
Describe the use of Windows Server Update Services.
Manage updates using WSUS.